ARTICLE APPEARED ON PAGE 43

NEWSWEEK
12 November 1979

P-Morgenthau, Tom
P-MARTIN, DAVID C.
P-Shannon, Elaine
ORGI IBM
CIA 3.01 (Industrial)
CIA 4-01 Business
Coing under Morgenthau)

NATIONAL AFFAIRS

SPYING ON U.S. BUSINESS

As in most real-life espionage stories, the details are hazy even now. But sometime in the early 1970s, U.S. intelligence officials say, a train carrying an IBM 370 computer sold to Poland by a European firm mysteriously broke down along the border between Poland and the Soviet Union. When the train began rolling again, the computer was no longer aboard. In March 1973, officials say, Soviet authorities contacted a European computer firm to buy spare parts for an IBM 370. The parts were available, they were told, but the firm needed to know the serial number of the computer. Sure enough, the serial number turned out to be that of the missing IBM 370—then among the most sophisticated computers in the world.

The computer's apparent diversion into Russian hands is an extreme case—but in many less dramatic ways, U.S. officials believe, the Soviet Union is stepping up its attempts to steal U.S. military and technological secrets by penetrating American industry. "We can lock up everything in the Pentagon," says FBI chief William Webster, "but the same information may be in a safe in a company building" where it is "much more vulnerable." Safeguarding those secrets is a gargantuan task: some 11,000 firms have access to classified defense information, and about 120,000 of their employees have top-secret clearances. Both the FBI and the Central Intelligence Agency intensified security checks of industrial firms—but CIA director Stansfield Turner termed the CIA's findings "discouraging." Soviet snoops are assumed to monitor communications at major defense plants, and last February six Boeing Co. employees lost their security clearances because they carelessly sent information about the MX missile over an ordinary phone line.

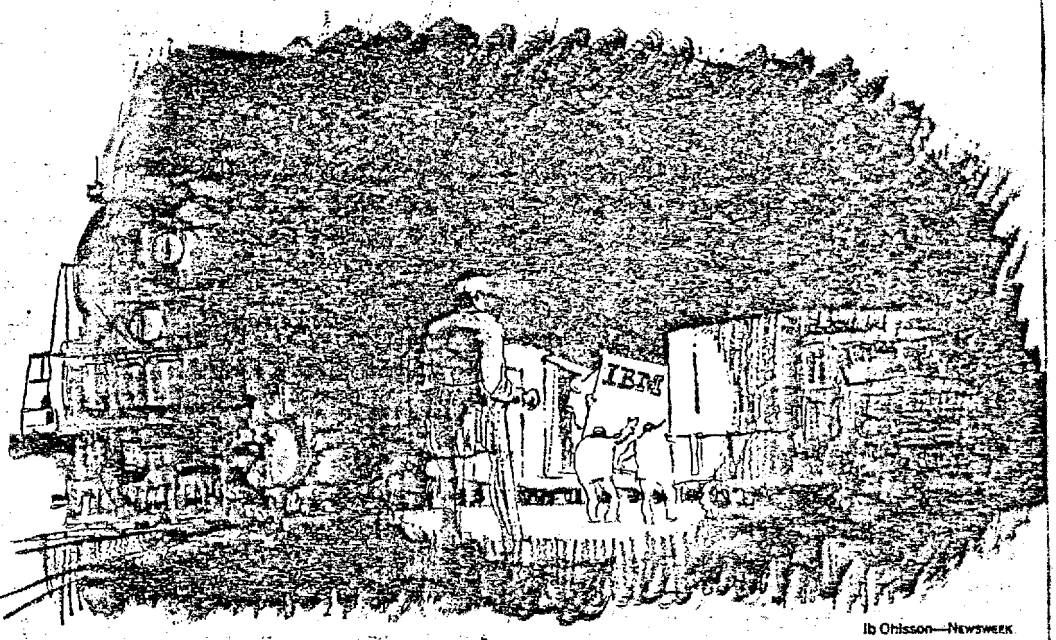
BRIBES: The Soviet-bloc countries employ a wide range of techniques to crib American technological innovations. FBI agents in Chicago, for example, are investigating a case in which the Polish Government apparently set up a dummy corporation to acquire industrial data that had been embargoed for export to Communist countries. And a Reston, Va., computer firm told the FBI in September that one of its executives had been offered a $500,000 bribe by a Soviet agent for a copy of an unclassified bit of software used to program the computers of a number of major corporations, including Gulf Oil and Citibank. Companies in financial trouble are special targets for foreign strings attached may not be obvious at first," an FBI official says. "Nevertheless, the businessman is slowly drawn into a foreign intelligence network."

Knowledgeable spies can reap a rich harvest of advanced technical data without resorting to skulduggery. The Soviets, for example, subscribe to a biweekly report on current scientific research published by the government-run National Technical Information Service. It collates only unclassified research, but some of the papers provide valuable technical clues—"a running account of the level of U.S. technology on a very, very timely basis," says one U.S. expert. The Soviet Union has a standing request to receive microfilm copies of all documents relating to such fields as "missile technology" and "optics and lasers." Inevitably, a document or two turns out to have been improperly declassified.

Similarly, participants in scientific meetings that routinely include Soviet experts often seem "lax . . . about the protection of militarily significant technologies," complains J. Fred Bucy, president of Texas Instruments. And Webster is concerned by the influx of visiting scientists and businessmen from the Communist bloc. One Hungarian physicist was allowed to study magnetic-bubble memories for computers—until a defector revealed the Hungarian had a deadline for delivering a prototype to Moscow.

Controlling the spread of sophisticated American technology becomes more difficult because the Soviet espionage campaign now aims to copy both the product and the manufacturing process. The CIA has found, for example, that the microcircuitry inside a Soviet electronic calculator duplicated that of an American-made model—a relatively simple bit of "reverse engineering." But U.S. experts were disturbed that the Soviets had also obtained advanced American-made equipment to manufacture the microcircuits, probably through a legal sale to Yugoslavia.

Stemming the steady leakage of American technology poses a series of policy dilemmas for U.S. officials. It is one thing to crack down on espionage or illegal sales. But many American advances are there for the asking. Sophisticated technology is America's most competitive export on the world market, and the free exchange of technical information is highly valued by scientists. The Soviet bloc's access to scientific research can be eliminated only by suppressing scientific debate and business enterprise—and so far no one seems willing



Ib Ohlsson—Newsweek

An IBM 370 disappears in Poland: Stepped-up efforts to steal U.S. technological secrets